R E P U B L I Q U E F R A N Ç A I S E PCT/EP2004/051144

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REC'D 26 AUG 2004
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

BEST AVAILABLE COPY

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 30 JUIN 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

M Heuct

Martine PLANCHE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Important ! Remplir impérativement la 2ème page.

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W /190600

Réservé à l'INPI	
REMISE DES PIÈCES DATE	18 JUIN 2003
LIEU	INPI PARIS F
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI	03 07379
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI	18 JUIN 2003
Vos références pour ce dossier (facultatif)	GEM 1511

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

GEMPLUS
LA VIGIE
Département Brevets
BP 90
13705 LA CIOTAT CEDEX

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes	
Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date / /
ou demande de certificat d'utilité initiale	N°	Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE CONTRE-MESURE PAR MASQUAGE DE L'ACCUMULATEUR DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR		☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»	
Nom ou dénomination sociale		GEMPLUS	
Prénoms			
Forme juridique		S.A	
N° SIREN		3 4 9 7 1 1 2 0 0	
Code APE-NAF		3 2 1 B	
Adresse	Rue	Avenue du Pic de Bertagne Parc d'activités de Gémenos	
	Code postal et ville	13420	GEMENOS
Pays		FRANCE	
Nationalité		FRANCE	
N° de téléphone (facultatif)		04 42 36 53 50	
N° de télécopie (facultatif)		04 42 36 63 43	
Adresse électronique (facultatif)		alisee.couteau@gemplus.com	

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI	
REMISE DES PIÈCES DATE	18 JUIN 2003
LIEU	INPI PARIS F
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI	03 07379

DB 540 W /190600

Vos références pour ce dossier : *(facultatif)*	GEM 1511	
6 MANDATAIRE		
Nom	BRUYERE	
Prénom	Pierre	
Cabinet ou Société	GEMPLUS	
N °de pouvoir permanent et/ou de lien contractuel	11535 et délégation 11571	
Adresse — Rue	LA VIGIE Dpt Brevets - BP 90	
Adresse — Code postal et ville	13705	LA CIOTAT CEDEX
N° de téléphone *(facultatif)*	04 42 36 53 50	
N° de télécopie *(facultatif)*	04 42 36 63 43	
Adresse électronique *(facultatif)*	alisee.couteau@gemplus.com	
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs	☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**	
8 RAPPORT DE RECHERCHE	**Uniquement pour une demande de brevet (y compris division et transformation)**	
Établissement immédiat ou établissement différé	☒ ☐	
Paiement échelonné de la redevance	**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non	
9 RÉDUCTION DU TAUX DES REDEVANCES	**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Pierre BRUYERE Ingénieur Brevets Pierre Bruy	**VISA DE LA PRÉFECTURE OU DE L'INPI**

PROCEDE DE CONTRE-MESURE PAR MASQUAGE DE L'ACCUMULATEUR DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme cryptographique à clé publique.

Dans le modèle classique de la cryptographie à clé secrète, deux personnes désirant communiquer par l'intermédiaire d'un canal non sécurisé doivent au préalable se mettre d'accord sur une clé secrète de chiffrement K. La fonction de chiffrement et la fonction de déchiffrement utilisent la même clé K. L'inconvénient du système de chiffrement à clé secrète est que ledit système requiert la communication préalable de la clé K entre les deux personnes par l'intermédiaire d'un canal sécurisé, avant qu'un quelconque message chiffré ne soit envoyé à travers le canal non sécurisé. Dans la pratique, il est généralement difficile de trouver un canal de communication parfaitement sécurisé, surtout si la distance séparant les deux personnes est importante. On entend par canal sécurisé un canal pour lequel il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites personnes.

Le concept de cryptographie à clé publique fut inventé par Whitfield Diffie et Martin Hellman en 1976 (IEEE Transactions on Information Theory, volume 22, numéro 6, pages 644-654, 1976). La cryptographie à clé publique permet de résoudre le problème de la distribution des clés à travers un canal non sécurisé. La cryptographie à clé publique est basée sur la difficulté de résoudre certains problèmes (supposés) calculatoirement infaisables. Le problème considéré par Diffie et Hellman est la résolution du logarithme discret dans le groupe multiplicatif d'un corps fini.

On rappelle que dans un corps fini, le nombre d'éléments du corps s'exprime toujours sous la forme q^n, où q est un nombre premier appelé la caractéristique du corps et n est un nombre entier. Un corps fini possédant q^n éléments est noté GF(q^n). Dans le cas où le nombre entier n est égal à 1, le corps fini est dit premier. Un corps possède deux groupes : un groupe multiplicatif et un groupe additif. Dans le groupe multiplicatif, l'élément neutre est noté 1 et la loi de groupe est notée multiplicativement par le symbole . et est appelée multiplication. Cette loi définit l'opération d'exponentiation dans le groupe multiplicatif G: étant donné un élément g appartenant à G et un entier d, le résultat de l'exponentiation de g par d est l'élément y tel que $y=g^d=g.g.g.\ldots.g$ (d fois) dans le groupe G.

Le problème du logarithme discret dans le groupe multiplicatif G d'un corps fini consiste à trouver, s'il existe, un entier d tel y=g^d, étant donné deux éléments y et g appartenant à G.

Ainsi, il est possible pour deux personnes de construire une clé commune K. Une personne A choisit un nombre aléatoire a, calcule la demi-clé K_a=g^a dans G et envoie K_a à une personne B. De la même façon, B choisit un nombre aléatoire b, calcule la demi-clé K_b=g^b dans G et envoie K_b à A. Ensuite, A calcule K=K_b^a et B calcule K=K_a^b. De façon remarquable, seules les personnes A et B sont capables de construire la clé commune K=g^(ab).

En plus de l'échange de clés, la cryptographie à clé publique permet le chiffrement des données, la signature numérique, l'authentification ou l'identification. De nombreux systèmes cryptographiques basés sur le problème du logarithme discret sont présentés dans « Handbook of Applied Cryptography » par Alfred Menezes, Paul van

Oorschot et Scott Vanstone, CRC Press, 1997. On note à titre d'exemple le chiffrement d'El Gamal ou la signature numérique DSA.

D'autres groupes ont été envisagés pour implémenter des analogues aux systèmes cryptographiques construits dans le groupe multiplicatif d'un corps fini. En 1985, Victor Miller et Neal Koblitz ont indépendamment proposé l'utilisation de courbes elliptiques dans des systèmes cryptographiques. L'avantage de systèmes cryptographiques à base des courbe elliptiques est qu'ils fournissent une sécurité équivalente aux autres systèmes cryptographiques mais avec des tailles de clé moindres. Ce gain en taille de clé implique une diminution des besoins en mémoire et une réduction des temps de calcul, ce qui rend l'utilisation des courbes elliptiques particulièrement adaptées pour des applications de type carte à puce.

Pour mémoire, une courbe elliptique sur un corps fini GF(q^n) est l'ensemble des points (x,y) appartenant à GF(q^n) vérifiant l'équation :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \text{ , avec } a_i \text{ dans } GF(q^n)$$

et du point à l'infini O. Toute courbe elliptique sur un corps peut s'exprimer sous cette forme.

L'ensemble des points (x,y) et le point à l'infini forment un groupe abélien, dans lequel le point à l'infini est l'élément neutre et dans lequel l'opération de groupe est l'addition de points, notée + et donnée par la règle bien connue de la sécante et de la tangente (voir par exemple « Elliptic Curve Public Key Cryptosystems » par Alfred Menezes, Kluwer, 1993). Dans ce groupe, la paire (x,y), où l'abscisse x et l'ordonnée y sont des éléments du corps GF(q^n), forme les coordonnées affines d'un point P de la courbe elliptique.

Il existe 2 procédés pour représenter un point d'une courbe elliptique :

- Premièrement, la représentation en coordonnées affines ; dans ce procédé, un point P de la courbe elliptique est représenté par ses coordonnées (x,y) ;
- Deuxièment, la représentation en coordonnées projectives.

L'avantage de la représentation en coordonnées projectives est qu'elle permet d'éviter les divisions dans le corps fini, lesdites divisions étant les opérations les plus coûteuses en temps de calcul.

La représentation en coordonnés projectives la plus couramment utilisée, dite jacobienne, est celle consistant à représenter un point P de coordonnées affines (x,y) sur la courbe elliptique par les coordonnées (X,Y,Z), telles que x=X/Z^2 et y=Y/Z^3. La représentation jacobienne d'un point n'est pas unique parce que le triplet (X,Y,Z) et le triplet (λ^2.X, λ^3.Y, λ.Z) représentent le même point quel que soit l'élément non-nul λ appartenant au corps fini sur lequel est défini la courbe elliptique.

Une autre représentation en coordonnées projectives, dite homogène, consiste à représenter un point P de coordonnées affines (x,y) sur la courbe elliptique par les coordonnées (X,Y,Z), telles que x=X/Z et y=Y/Z. La représentation homogène d'un point n'est pas unique parce que le triplet (X,Y,Z) et le triplet (λ.X, λ.Y, λ.Z) représentent le même point quel que soit l'élément non-nul λ appartenant au corps fini sur lequel est défini la courbe elliptique.

L'opération d'addition de points permet de définir une opération d'exponentiation sur courbe elliptique : étant donné un point P appartenant à une courbe elliptique et un entier d, le résultat de l'exponentiation de P par d est le point Q tel que Q=d*P=P+P+...+P (d fois). Dans le cas des courbes elliptiques, afin d'insister sur la notation additive, l'exponentiation est encore appelée multiplication scalaire.

La sécurité des algorithmes de cryptographie sur courbes elliptiques est basée sur la difficulté du problème du logarithme discret dans le groupe G formé par les points d'une courbe elliptique, ledit problème consistant à partir de deux points Q et P appartenant à G, de trouver, s'il existe, un entier d tel que Q=d*P.

Il existe de nombreux algorithmes cryptographiques basés sur le problème du logarithme discret. Ainsi, il est possible de mettre en œuvre des algorithmes assurant l'authentification, la confidentialité, le contrôle d'intégrité et l'échange de clé.

Un point commun à la plupart des algorithmes cryptographiques basés sur le problème du logarithme discret dans un groupe G est qu'ils comprennent comme paramètre un élément g appartenant à ce groupe. La clé privée est un entier d choisi aléatoirement. La clé publique est un élément y tel que y=g^d. Ces algorithmes cryptographiques font généralement intervenir une exponentiation dans le calcul d'un élément z=h^d où d est la clé secrète et h est un élément du groupe G.

Dans le paragraphe ci-dessous, on décrit un algorithme de chiffrement basé sur le problème du logarithme discret

dans un groupe G, noté multiplicativement. Ce schéma est analogue au schéma de chiffrement d'El Gamal. Soient un groupe G et un élément g dans G. La clé publique de chiffrement est y=g^d et la clé privée de déchiffrement est d. Un message m est chiffré de la manière suivante.

Le chiffreur, ou personne désirant chiffrer un message, choisit un entier k aléatoirement et calcule les éléments h=g^k et z=y^k dans le groupe G, et c=R(z)⊕ m où R est une fonction appliquant les éléments de G sur l'ensemble des messages et ⊕ désigne l'opérateur du OU exclusif. Le chiffré correspondant à m est la paire (h,c).

Le déchiffreur, ou personne désirant déchiffrer un message, qui possède la clé secrète d déchiffre m en calculant :

z'=h^d=g^(k.d)=y^k et m=R(z')⊕ c.

Pour réaliser les exponentiations nécessaires dans les procédés de calcul décrits précédemment, plusieurs algorithmes existent :

- algorithme d'exponentiation binaire gauche-droite;
- algorithme d'exponentiation k-aire gauche-droite;
- algorithme d'exponentiation modifié k-aire gauche-droite;
- algorithme d'exponentiation avec fenêtres glissantes gauche-droite ;
- algorithme d'exponentiation en représentation signée de l'exposant.

Ces algorithmes sont détaillés dans le chapitre 14 de « Handbook of Applied Cryptography » par A.J. Menezes, P.C. van Oorschot et S.A. Vanstone, CRC Press, 1997. Cette liste n'est pas exhaustive.

L'algorithme le plus simple et le plus utilisé est l'algorithme d'exponentiation binaire gauche-droite. L'algorithme d'exponentiation binaire gauche-droite prend en entrée un élément g d'un groupe G et un exposant d. L'exposant d est noté $d=(d(t),d(t-1),\ldots,d(0))$, où $(d(t),d(t-1),\ldots,d(0))$ est la représentation binaire de d, avec $d(t)$ le bit le plus significatif et $d(0)$ le bit le moins significatif. L'algorithme retourne en sortie l'élément $y=g^d$ dans le groupe G.

L'algorithme d'exponentiation binaire gauche-droite comporte les 3 étapes suivantes :

1) Initialiser le registre A avec l'élément neutre de G
2) Pour i allant de t à 0 exécuter :
2a) Remplacer A par A^2
2b) Si $d(i)=1$ remplacer A par A.g
3) Retourner A.

L'algorithme d'exponentiation k-aire gauche-droite prend en entrée un élément g d'un groupe G et un exposant d noté $d=(d(t),d(t-1),\ldots, d(0))$, où $(d(t),d(t-1),\ldots,d(0))$ est la représentation k-aire de d, c'est-à-dire chaque chiffre $d(i)$ de la représentation de d est un entier compris entre 0 et 2^k-1 pour un entier $k\geq1$, avec $d(t)$ le chiffre le plus significatif et $d(0)$ le chiffre le moins significatif. L'algorithme retourne en sortie l'élément $y=g^d$ dans le groupe G et comporte les 4 étapes suivantes :

1) Précalculs :
1a) Définir $g_1=g$
1b) Si $k\geq2$, pour i allant de 2 à (2^k-1) : calculer $g_i=g^i$

2) Initialiser le registre A avec l'élément neutre de G

3) Pour i allant de t à 0 exécuter :

3a) Remplacer A par A^(2^k)

3b) Si d(i) est non-nul, remplacer A par A.g_i

4) Retourner A.

Dans le cas où k est égal à 1, on remarque que l'algorithme d'exponentiation k-aire gauche-droite n'est autre que l'algorithme d'exponentiation binaire gauche-droite.

L'algorithme d'exponentiation k-aire gauche-droite peut être adapté pour prendre en entrée une représentation signée de l'exposant d. L'exposant d est donné par la représentation (d(t),d(t-1),…,d(0)) dans laquelle chaque chiffre d(i) est un entier compris entre -(2^k-1) et 2^k-1 pour un entier k≥1, avec d(t) le chiffre le plus significatif et d(0) le chiffre le moins significatif. L'étape 3b de l'algorithme précédent est alors remplacée par

3b') Si d(i) est strictement positif, remplacer A par A.g_i ; et si d(i) est strictement négatif, remplacer A par A.(g_i)^(-1)

Cette adaptation est particulièrement intéressante quand l'inverse des éléments g_i, noté (g_i)^(-1), est facile ou peu coûteux à calculer. Ceci est par exemple le cas dans le groupe G des points d'une courbe elliptique. Dans le cas où l'inverse des éléments g_i n'est pas facile ou trop coûteux à calculer, leur valeur est précalculée.

L'algorithme d'exponentiation modifié k-aire gauche-droite réduit les précalculs de l'algorithme d'exponentiation k-aire gauche-droite en ne calculant que g^2 et les

puissances impaires de g lorsque $k \geq 2$. Il a les mêmes entrées que l'algorithme d'exponentiation k-aire gauche-droite et retourne en sortie l'élément $y=g^d$ dans le groupe G. Il comporte les 4 étapes suivantes :

1) Précalculs :
   1a) Définir $g_1 = g$ et calculer $g_2=g^2$
   1b) Pour i allant de 1 à $(2^{(k-1)}-1)$: calculer $g_{2i+1}=g^{(2i+1)}$
2) Initialiser le registre A avec l'élément neutre de G
3) Pour i allant de t à 0 exécuter :
   3a) Si $d(i)=0$, remplacer A par $A^{(2^k)}$
   3b) Si d(i) est non-nul, écrire $d(i)=2^v.u$ avec u impair et remplacer A par $[A^{(2^{(k-v)})}.g_u]^{(2^v)}$
4) Retourner A.

Tout comme l'algorithme d'exponentiation modifié k-aire gauche-droite, l'algorithme d'exponentiation avec fenêtres glissantes gauche-droite réduit non seulement les précalculs mais aussi le nombre moyen de multiplications dans le groupe G. Il prend en entrée un élément g d'un groupe G, un exposant d, noté $d=(d(t),d(t-1),\ldots,d(0))$, où $(d(t),d(t-1),\ldots,d(0))$ est la représentation binaire de d et un entier $k>1$ appelé la largeur de la fenêtre. Il retourne en sortie l'élément $y=g^d$ dans le groupe G et comporte les 4 étapes suivantes :

1) Précalculs :
   1a) Définir $g_1 = g$ et calculer $g_2=g^2$
   1b) Pour i allant de 1 à $(2^{(k-1)}-1)$: calculer $g_{2i+1}=g^{(2i+1)}$
2) Initialiser le registre A avec l'élément neutre de G et le compteur i avec la valeur t
3) Tant que i est positif ou nul exécuter :

3a) Si $d(i)=0$, remplacer A par A^2 et i par i-1

3b) Si $d(i)=1$, exécuter :

3b-1) Trouver la plus longue chaîne binaire $d(i), d(i-1), \ldots, d(j)$ telle que $i-j+1 \leq k$ et $d(j)=1$

3b-2) Définir u comme l'entier ayant pour représentation binaire $(d(i), d(i-1), \ldots, d(j))$

3b-3) Remplacer A par $A\hat{}(2\hat{}(i-j+1)).g_u$ et i par j-1

4) Retourner A.

Les algorithmes d'exponentiation pour le calcul de y=g^d dans le groupe G décrits précédemment ainsi que leurs nombreuses variantes parcourt l'exposant d de la gauche vers la droite, c'est-à-dire de la position la plus significative vers la position la moins significative. De façon remarquable, on distingue deux types d'opérations :

- Les multiplications du registre A, appelé accumulateur, par lui-même ;
- Les multiplications du registre A par la valeur constante g ou une de ses puissances $g_i=g\hat{}i$.

Lorsque g (respectivement une des ses puissances g_i) présente une structure particulière, la multiplication de l'accumulateur A par g dans le groupe G (respectivement une de ses puissances g_i) peut être substantiellement plus rapide que la multiplication de deux éléments arbitraires de G.

Notamment, lorsque le groupe G est le groupe multiplicatif du corps premier GF(q) et que g (respectivement une de ses puissances g_i) est représenté comme un entier en simple précision, le calcul de A.g (respectivement A.gi) en multi-précision dans G peut se faire en un temps linéaire. Par exemple, si g est égal à 2, la multiplication de A par g=2

revient à additionner A avec lui-même dans le groupe G : A.2=A+A.

Les algorithmes d'exponentiation décrits précédemment sont donnés en notation multiplicative ; en d'autres mots, la loi de groupe du groupe G est notée . (multiplication). Ces algorithmes peuvent être données en notation additive en remplaçant les multiplications par des additions ; en d'autres mots, la loi de groupe du groupe G est notée + (addition). Ceci est par exemple le cas du groupe des points d'une courbe elliptique qui est le plus souvent donné sous forme additive. Dans ce cas, le cas de Q=d*P sur une courbe elliptique peut se calculer par n'importe lequel des algorithmes décrits précédemment en remplaçant l'opération de multiplication par l'addition de points sur ladite courbe elliptique. Similairement et de façon remarquable, on distingue deux types d'opérations :

- Les additions du registre A, appelé accumulateur, par lui-même ;
- Les additions du registre A par la valeur constante P ou un de ses multiples P_i=i*P.

Lorsque le point P (respectivement une des ses multiples P_i) a une structure particulière, l'addition de l'accumulateur A par P (respectivement un de ses multiples P_i) peut être substantiellement plus rapide que l'addition de deux points arbitraires sur une courbe elliptique. Notamment, si le point P est représenté en coordonnées projectives (de façon jacobienne ou homogène) par P=(X,Y,Z) avec la coordonnée en Z égale à 1, le nombre d'opérations pour calculer l'addition des points A et P en coordonnées projectives est réduit.

Il est apparu que l'implémentation sur carte à puce d'un algorithme cryptographique à clé publique basé sur le

logarithme discret était vulnérable à des attaques consistant en une analyse différentielle d'une grandeur physique permettant de retrouver la clé secrète. Ces attaques sont appelées attaques de type DPA, acronyme pour Differential Power Analysis et ont notamment été dévoilées par Paul Kocher (Advances in Cryptology - CRYPTO '99, volume 1966 de Lecture Notes in Computer Science, pages 388-397, Springer-Verlag, 1999). Parmi les grandeurs physiques qui peuvent être exploitées à ces fins, on peut citer la consommation en courant, le champ électromagnétique ... Ces attaques sont basées sur le fait que la manipulation d'un bit, c'est à dire son traitement par une instruction particulière, a une empreinte particulière sur la grandeur physique considérée selon sa valeur.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le microprocesseur du composant électronique lors de l'exécution d'un algorithme cryptographique. Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme cryptographique, rendant le système cryptographique vulnérable.

Une parade efficace aux attaques de type DPA est de rendre aléatoire les entrées de l'algorithme d'exponentiation utilisé pour calculer y=g^d. En d'autres termes, il s'agit de rendre l'exposant d et/ou l'élément g aléatoire. En notation additive,

dans le calcul de Q=d*P, il s'agit de rendre l'exposant d et/ou l'élément P aléatoire.

Des procédés de contre-mesure appliquant ce principe sont connus. De tels procédés de contre-mesure sont notamment décrits dans un article de Jean-Sébastien Coron (Cryptographic Hardware and Embedded Systems, volume 1717 de Lecture Notes in Computer Science, pages 292-302, Springer-Verlag, 1999).

Notamment, dans cet article, un procédé de contre-mesure consiste à masquer le point P du groupe des points d'une courbe elliptique définie sur le corps GF(q^n) en utilisant des coordonnées projectives de ce point, définies de façon aléatoire. Dans l'article précité, on tire ainsi un nombre aléatoire λ non-nul dans GF(q^n) et on représente le point P=(x,y) par des coordonnées projectives fonction de ce nombre aléatoire, par exemple sous la forme P=(λ^2.x, λ^3.y,λ) en représentation jacobienne, ou P=(λ.x, λ.y, λ) en représentation homogène. On applique l'algorithme d'exponentiation à ces coordonnées. On obtient une représentation du point Q en coordonnées projectives, desquelles on déduit (calcule) les coordonnées affines de ce point.

Un autre procédé de contre-mesure connu par l'homme du métier pour masquer l'élément g du groupe multiplicatif G d'un corps fini GF(q^n) consiste à représenter cet élément dans une extension de GF(q^n), de façon aléatoire. Par exemple, dans le cas d'un corps premier GF(q), une extension de GF(q) est donnée par l'anneau R=Z/(qk) obtenu en quotientant l'anneau des entiers Z par l'anneau qkZ pour un entier k donné. On tire alors un nombre aléatoire λ dans l'anneau Z/(k) et on représente l'élément g par g^*=g+λ.q. On applique l'algorithme d'exponentiation à l'élément g^* dans R et on obtient une représentation de l'élément y^*=(g^*)^d dans R, de laquelle on déduit (calcule) la valeur de y=g^d dans G en réduisant y^* modulo q.

Ce procédé de contre-mesure s'applique également dans le cas d'un élément g du groupe multiplicatif G d'un corps fini GF(q^n) avec n>1. Si le corps GF(q^n) est représenté comme le quotient de l'anneau polynomial GF(q)[X] par un polynôme irréductible p de degré n sur GF(q), alors une extension de GF(q^n) est donnée par l'anneau R=GF(q)[X]/(p.k) obtenu en quotientant l'anneau polynomial GF(q)[X] par le produit des polynômes p et k avec k donné. On tire alors un polynôme aléatoire $\lambda(X)$ dans l'anneau GF[X]/(k) et on représente l'élément g par $g^*=g+\lambda.p$. On applique l'algorithme d'exponentiation à l'élément g^* dans R et on obtient une représentation de l'élément $y^*=(g^*)$^d dans R, de laquelle on déduit (calcule) la valeur de y=g^d dans G en réduisant y^* modulo p(X).

L'inconvénient de l'ensemble de ces procédés rendant aléatoire g ou P décrits ci-dessus est que si l'élément g (respectivement P) du groupe G est rendu aléatoire dans le calcul de y=g^d (respectivement Q=d*P), alors la structure particulière de g (respectivement P) ne peut plus être exploitée pour accélérer ledit calcul.

Un objet de la présente invention est un procédé de contre-mesure, notamment vis à vis des attaques de type DPA.

Un autre objet de l'invention est un procédé de contre-mesure aisé à mettre en oeuvre.

Par rapport aux procédés de contre-mesure connus, le procédé proposé présente l'avantage d'être plus rapide pour protéger l'évaluation de y=g^d dans un groupe G noté de façon multiplicative (respectivement l'évaluation de Q=d*P si le groupe est noté de façon additive) lorsque l'algorithme d'exponentiation utilisé pour ce calcul est de type gauche-droite et que g

(respectivement P) a une structure particulière ; les algorithmes d'exponentiation gauche-droite ayant la propriété remarquable d'avoir des opérations de multiplication de l'accumulateur A par la valeur constante g ou une de ses puissances g_i=g^i (respectivement des opérations d'addition de l'accumulateur A par la valeur constante P ou un de ses multiples P_i=i*P).

L'idée à la base de l'invention est de rendre aléatoire l'accumulateur A dans l'algorithme d'exponentiation gauche-droite utilisé. Ce procédé de masquage peut se faire au début de l'algorithme ou encore de façon déterministe ou probabiliste durant l'exécution de l'algorithme. Ainsi le calcul de y=g^d dans le groupe G noté de façon multiplicative (respectivement Q=d*P si le groupe G est noté de façon multiplicative) est rendu aléatoire sans que la structure de l'élément g (respectivement P) ou une de ses puissances g_i=g^i (respectivement un de ses multiples P_i=i*P) ne soit altérée.

L'invention concerne donc un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé publique, comprenant un calcul d'exponentiation, avec un algorithme d'exponentiation de type gauche-droite, de type y=g^d où g et y sont des éléments du groupe déterminé G noté de façon multiplicative et d est un nombre prédéterminé, caractérisé en ce qu'il comprend une étape de tirage aléatoire, au début ou durant l'exécution dudit algorithme d'exponentiation, de façon déterministe ou probabiliste, pour masquer l'accumulateur A de sorte que la structure de l'élément g ou une de ses puissances g_i=g^i ne soit pas altérée. Ce procédé s'applique de la même façon si le groupe G est noté de façon additive.

D'autres caractéristiques et avantages de l'invention sont présentées dans les descriptions suivantes, faites en référence à des modes de réalisation particuliers.

On a vu que l'algorithme d'exponentiation le plus simple et le plus utilisé dans un groupe G est l'algorithme d'exponentiation binaire gauche-droite et que ce type d'algorithme est plus efficace lorsque l'élément de G en entrée a une structure particulière. Par ailleurs, la plupart des systèmes cryptographiques dont la sécurité est basée sur le problème du logarithme discret sont construits dans le groupe multiplicatif d'un corps fini GF(q) avec q premier ou dans le groupe des points d'une courbe elliptique définie sur un corps fini.

Soit donc G le groupe multiplicatif d'un corps fini GF(q) avec q premier et soit un algorithme d'exponentiation binaire gauche-droite prenant en entrée un élément g de G représenté comme un entier en simple précision et un exposant d donné par la représentation binaire (d(t),d(t-1),...,d(0)), et retournant en sortie l'élément y=g^d dans le groupe G. Dans l'invention, l'accumulateur dudit algorithme d'exponentiation est masqué de façon aléatoire. Ainsi, un procédé de contre-mesure selon l'invention appliqué au groupe multiplicatif G d'un corps premier GF(q) peut s'écrire comme suit :

1) Déterminer un entier k définissant la sécurité du masquage
2) Initialiser l'accumulateur A avec l'entier 1
3) Pour i allant de t à 0, exécuter :
3a) Tirer un entier aléatoire λ compris entre 0 et k-1 et remplacer l'accumulateur A par A+λ.q (modulo k.q)
3b) Remplacer A par A^2 (modulo k.q)
3c) Si d(i)=1 remplacer A par A.g (modulo k.q)
4) Retourner A (modulo q).

Typiquemment, le paramètre de sécurité k est fixé à 32 ou 64 bits. De façon remarquable à l'étape 3c, la multiplication se fait avec l'entier g représenté en simple précision.

De préférence, le masquage de l'accumulateur A à l'étape 3a ne se fait qu'au début de l'exponentiation. On obtient ainsi le procédé de contre-mesure suivant :

1) Déterminer un entier k définissant la sécurité du masquage
2) Tirer un entier aléatoire λ compris entre 0 et k-1 et initialiser l'accumulateur A avec l'entier $1+\lambda.q$ (modulo k.q)
3) Pour i allant de t-1 à 0, exécuter :
3a) Remplacer A par A^2 (modulo k.q)
3b) Si d(i)=1 remplacer A par A.g (modulo k.q)
4) Retourner A (modulo q).

De façon remarquable à l'étape 3b, la multiplication se fait avec l'entier g représenté en simple précision.

Une autre application intéressante de l'invention concerne l'exponentation dans le groupe G des points d'une courbe elliptique définie sur un corps fini GF(q^n). Dans ce groupe G, noté de façon additive, l'inversion d'un point P, notée -P, est une opération peu coûteuse de sorte qu'il est intéressant de remplacer l'algorithme d'exponentiation binaire gauche-droite par sa version signée comme expliqué dans un article de François Morain et de Jorge Olivos (Theoretical Informatics and Applications, volume 24, pages 531–543, 1990). Soit donc G le groupe des points d'une courbe elliptique définie sur un corps fini GF(q^n) et soit un algorithme d'exponentiation binaire signé gauche-droite prenant en entrée un point P représenté en coordonnées affines par P=(x,y) et un exposant d donné par la représentation binaire signée (d(t+1),d(t),…,d(0)) avec d(i)=0, 1

ou -1 pour $0 \le i \le t$ et $d(t+1)=1$, et retournant en sortie le point $Q=d*P$ dans le groupe G en coordonnées affines. Dans l'invention, l'accumulateur dudit algorithme d'exponentiation est un triplet de valeurs dans GF(q^n) et est masqué de façon aléatoire. Ainsi, un procédé de contre-mesure selon l'invention appliqué au groupe G des points d'une courbe elliptique définie sur un corps fini GF(q^n) peut s'écrire comme suit :

1) I Initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet $(x,y,1)$

2) Pour i allant de t à 0, exécuter :

2a) Tirer un élément non nul aléatoire λ dans GF(q^n) et remplacer l'accumulateur $A=(A_X,A_Y,A_Z)$ par $(\lambda^2.A_X,\lambda^3.A_Y, \lambda.A_Z)$

2b) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation jacobienne, sur la courbe elliptique

2c) Si d(i) est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation jacobienne, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/(A_Z)^2, A_Y/(A_Z)^3)$.

De façon remarquable à l'étape 2c, l'addition sur la courbe elliptique se fait avec le point $P=(x,y,1)$ dont la coordonnée en Z est égale à 1.

De préférence, le masquage de l'accumulateur A à l'étape 2a ne se fait qu'au début de l'exponentiation. On obtient ainsi le procédé de contre-mesure suivant :

1) Tirer un élément non nul aléatoire λ dans GF(q^n) et initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet (λ^2.x,λ^3.y, λ)

2) Pour i allant de t à 0, exécuter :

2a) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation jacobienne, sur la courbe elliptique

2b) Si d(i) est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation jacobienne, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/(A_Z)$^2, $A_Y/(A_Z)$^3).

De façon remarquable à l'étape 2b, l'addition sur la courbe elliptique se fait avec le point P=(x,y,1) dont la coordonnée en Z est égale à 1.

Si les points de la courbe elliptique sont représentés de façon homogène, les deux procédés de contre-mesure décrits précédemment deviennent respectivement :

1) Initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet (x,y,1)

2) Pour i allant de t à 0, exécuter :

2a) Tirer un élément non nul aléatoire λ dans GF(q^n) et remplacer l'accumulateur $A=(A_X,A_Y,A_Z)$ par $(\lambda.A_X,\lambda.A_Y,\lambda.A_Z)$

2b) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation homogène, sur la courbe elliptique

2c) Si d(i) est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation homogène, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/A_Z,\ A_Y/A_Z)$.

De façon remarquable à l'étape 2c, l'addition sur la courbe elliptique se fait avec le point $P=(x,y,1)$ dont la coordonnée en Z est égale à 1.

1) Tirer un élément non nul aléatoire λ dans GF(q^n) et initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet $(\lambda.x,\lambda.y,\ \lambda)$

2) Pour i allant de t à 0, exécuter :

2a) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation homogène, sur la courbe elliptique

2b) Si d(i) est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation homogène, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/A_Z,\ A_Y/A_Z)$.

De façon remarquable à l'étape 2b, l'addition sur la courbe elliptique se fait avec le point $P=(x,y,1)$ dont la coordonnée en Z est égale à 1.

De façon générale, le procédé de contre-mesure selon l'invention s'applique à tout algorithme d'exponentiation de type gauche-droite dans un groupe G, noté de façon multiplicative ou additive.

REVENDICATIONS

1. Procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme cryptographique à clé publique, comprenant un calcul d'exponentiation, avec un algorithme d'exponentiation de type gauche-droite, de type y=g^d où g et y sont des éléments du groupe déterminé G noté de façon multiplicative et d est un nombre prédéterminé, caractérisé en ce qu'il comprend une étape de tirage aléatoire, au début ou durant l'exécution dudit algorithme d'exponentiation de façon déterministe ou probabiliste, pour masquer l'accumulateur A.

2. Procédé de contre-mesure selon la revendication 1, caractérisé en ce que le groupe déterminé G est noté de façon additive.

3. Procédé de contre-mesure selon la revendication 1 caractérisé en ce que le groupe G est le groupe multiplicatif d'un corps fini noté GF(q^n), n étant un entier.

4. Procédé de contre-mesure selon la revendication 3 caractérisé en ce que l'entier est n égal à 1 : n=1.

5. Procédé de contre-mesure selon la revendication 4 caractérisé en ce qu'il comprend les étapes suivantes :
   1) Déterminer un entier k définissant la sécurité du masquage et donner d par la représentation binaire (d(t), d(t-1), ..., d(0)) ;
   2) Initialiser l'accumulateur A avec l'entier 1
   3) Pour i allant de t à 0, exécuter :
      3a) Tirer un entier aléatoire λ compris entre 0 et k-1 et remplacer l'accumulateur A par A+λ.q (modulo k.q)

3b) Remplacer A par A^2 (modulo k.q)

3c) Si d(i)=1 remplacer A par A.g (modulo k.q)

4) Retourner A (modulo q).

6. Procédé de contre-mesure selon la revendication 4 caractérisé en ce qu'il comprend les étapes suivantes :

1) Déterminer un entier k définissant la sécurité du masquage et donner d par la représentation binaire (d(t), d(t-1), …, d(0)) ;

2) Tirer un entier aléatoire λ compris entre 0 et k-1 et initialiser l'accumulateur A avec l'entier 1+λ.q (modulo k.q)

3) Pour i allant de t-1 à 0, exécuter :

3a) Remplacer A par A^2 (modulo k.q)

3b) Si d(i)=1 remplacer A par A.g (modulo k.q)

4) Retourner A (modulo q).

7. Procédé de contre-mesure selon la revendication 2 caractérisé en ce l'algorithme d'exponentiation s'applique au groupe G des points d'une courbe elliptique défini sur un corps fini GF(q^n).

8. Procédé de contre-mesure selon la revendication 7 caractérisé en ce qu'il comprend les étapes suivantes :

1) Initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet (x,y,1) et donner d par la représentation binaire signée (d(t+1), d(t), …, d(0)) avec d(t+1)=1;

2) Pour i allant de t à 0, exécuter :

2a) Tirer un élément non nul aléatoire λ dans GF(q^n) et remplacer l'accumulateur $A=(A_X,A_Y,A_Z)$ par $(\lambda\text{^}2.A_X, \lambda\text{^}3.A_Y, \lambda.A_Z)$

2b) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation jacobienne, sur la courbe elliptique

2c) Si $d(i)$ est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation jacobienne, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/(A_Z)\verb|^|2, A_Y/(A_Z)\verb|^|3)$.

9. Procédé de contre-mesure selon la revendication 7 caractérisé en ce qu'il comprend les étapes suivantes :

1) Tirer un élément non nul aléatoire λ dans GF(q^n), initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet $(\lambda\verb|^|2.x,\lambda\verb|^|3.y, \lambda)$ et donner d par la représentation binaire signée $(d(t+1), d(t), \ldots, d(0))$ avec $d(t+1)=1$;

2) Pour i allant de t à 0, exécuter :

2a) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation jacobienne, sur la courbe elliptique

2b) Si $d(i)$ est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation jacobienne, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/(A_Z)\verb|^|2, A_Y/(A_Z)\verb|^|3)$.

10. Procédé de contre-mesure selon la revendication 7 caractérisé en ce qu'il comprend les étapes suivantes :

1) Initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet $(x,y,1)$ et donner d par la représentation binaire signée $(d(t+1), d(t), \ldots, d(0))$ avec $d(t+1)=1$;

2) Pour i allant de t à 0, exécuter :

2a) Tirer un élément non nul aléatoire λ dans GF(q^n) et remplacer l'accumulateur $A=(A_X,A_Y,A_Z)$ par $(\lambda.A_X,\lambda.A_Y, \lambda.A_Z)$

2b) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation homogène, sur la courbe elliptique

2c) Si $d(i)$ est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation homogène, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/A_Z,\ A_Y/A_Z)$.

11. Procédé de contre-mesure selon la revendication 7 caractérisé en ce qu'il comprend les étapes suivantes :

1) Tirer un élément non nul aléatoire λ dans GF(q^n), initialiser l'accumulateur $A=(A_X,A_Y,A_Z)$ avec le triplet $(\lambda.x,\lambda.y,\ \lambda)$ et donner d par la représentation binaire signée $(d(t+1),\ d(t),\ \ldots,\ d(0))$ avec $d(t+1)=1$;

2) Pour i allant de t à 0, exécuter :

2a) Remplacer $A=(A_X,A_Y,A_Z)$ par $2*(A_X,A_Y,A_Z)$ en représentation homogène, sur la courbe elliptique

2b) Si $d(i)$ est non-nul remplacer $A=(A_X,A_Y,A_Z)$ par $(A_X,A_Y,A_Z)+d(i)*(x,y,1)$ en représentation homogène, sur la courbe elliptique

3) Si $A_Z=0$ retourner le point à l'infini ; sinon retourner $(A_X/A_Z,\ A_Y/A_Z)$.

12. Composant électronique utilisant le procédé de contre-mesure selon l'une quelconque des revendications précédentes.

reçue le 12/02/04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone :0 1 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa
N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé està remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	GEM 1511
N° D'ENREGISTREMENT NATIONAL	0307379,

TITRE DE L'INVENTION (200 caractères ou espaces maximum)
PROCEDE DE CONTRE-MESURE PAR MASQUAGE DE L'ACCUMULATEUR DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE

LE(S) DEMANDEUR(S) :
GEMPLUS
Avenue du Pic de Bertagne
Par d'activités de Gémenos
13420 GEMENOS

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		JOYE	
Prénoms		Marc	
Adresse	Rue	19 rue Voltaire	
	Code postal et ville	83640	SAINT ZACHARIE
Société d'appartenance *(facultatif)*		GEMPLUS	
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire) Pierre BRUYERE Ingénieur Brevets	Pierre Bruy